

**U.S. Department of Commerce
U.S. Patent and Trademark Office**



**Privacy Impact Assessment
for the
Data Conversion Laboratory Patent Support (DCLPS)**

Reviewed by: Henry J. Holcombe, Bureau Chief Privacy Officer

- ☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
Date: 2020.10.15 14:40:34 -04'00'

05/23/2020

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Data Conversion Laboratory Patent Support (DCLPS)

Unique Project Identifier: [2405] PTOC-027-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the system.

- (a) *Whether it is a general support system, major application, or other type of system*
The Data Conversion Laboratory Patent Support (DCLPS) is a general support system.
- (b) *System location*
The Data Conversion Laboratory Patent Support (DCLPS) is located in 6118 190 Street Suite 205 Fresh Meadows, NY 11365.
- (c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
The Data Conversion Laboratory Patent Support (DCLPS) is an external contractor system that has been implemented in support of the Continuous Data Conversion (CDC).
- (d) *The way the system operates to achieve the purpose(s) identified in Section 4*
The purpose of the system is to transform electronic Tagged Image File Format (TIFF) images of patent application documents to Extensible Markup Language (XML) documents based on a predefined XML schema.
- (e) *How information in the system is retrieved by the user*
The files in the new XML format allow patent examiners to search, manage, and manipulate different document types, using examination tools under development.
- (f) *How information is transmitted to and from the system*
DCL receives patent applications directly from the United States Patent and Trademark Office (USPTO). Data transfer between DCLPS and USPTO is done via a secure transport system. The transfers take place over public internet, from DCL to USPTO through their TIC (trusted internet connection).
- (g) *Any information sharing conducted by the system*
DCL does not share any information with other agencies, individuals, or organizations. The information provided by USPTO is used by DCL for authorized data conversion activities performed by internal personnel only.
- (h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
This PII and BII data is collected by the USPTO to enable identification of the inventory and facilitate the patent application process. It is provided to DCL so that data conversion activities can be performed on the collected patent application. The legal authority to collect PII and/or BII derives from 35 U.S.C. 1, 2 6, and 115; 5 U.S.C. 301 (SORN COMMERCE/PAT-TM-7).
- (i) *The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- ☐ This is a new information system.
- ☐ This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
j. Other changes that create new privacy risks (specify):					

- ☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*	<input type="checkbox"/>	e. File/Case ID	<input checked="" type="checkbox"/>	i. Credit Card	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
d. Employee ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: N/A					

General Personal Data (GPD)					
a. Name	<input checked="" type="checkbox"/>	g. Date of Birth	<input type="checkbox"/>	m. Religion	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	h. Place of Birth	<input type="checkbox"/>	n. Financial Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	i. Home Address	<input checked="" type="checkbox"/>	o. Medical Information	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	j. Telephone Number	<input checked="" type="checkbox"/>	p. Military Service	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	k. Email Address	<input checked="" type="checkbox"/>	q. Physical Characteristics	<input type="checkbox"/>

f. Race/Ethnicity	<input type="checkbox"/>	l. Education	<input type="checkbox"/>	r. Mother's Maiden Name	<input type="checkbox"/>
s. Other general personal data (specify): N/A					

Work-Related Data (WRD)					
a. Occupation	<input checked="" type="checkbox"/>	d. Telephone Number	<input checked="" type="checkbox"/>	g. Salary	<input type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	e. Email Address	<input checked="" type="checkbox"/>	h. Work History	<input type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	f. Business Associates	<input checked="" type="checkbox"/>		
i. Other work-related data (specify): N/A					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	<input type="checkbox"/>	d. Photographs	<input type="checkbox"/>	g. DNA Profiles	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	e. Scars, Marks, Tattoos	<input type="checkbox"/>	h. Retina/Iris Scans	<input type="checkbox"/>
c. Voice Recording/Signatures	<input type="checkbox"/>	f. Vascular Scan	<input type="checkbox"/>	i. Dental Profile	<input type="checkbox"/>
j. Other distinguishing features/biometrics (specify): N/A					

System Administration/Audit Data (SAAD)					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input checked="" type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	d. Queries Run	<input type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
g. Other system administration/audit data (specify): Hostname, event source, event type, event success or failure					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Data transfers between DCL and USPTO use the Cyclic Redundancy Check (CRC) against a checksum to validate the integrity. Least privilege, auditing, encryption at rest and transmission are used to maintain the integrity of the data and system.

2.4 Is the information covered by the Paperwork Reduction Act?

<input checked="" type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0021, 0651-0031, 0651-0032, and 0651-0033
<input type="checkbox"/>	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	--

Section 3: System Supported Activities3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
-------------------------------------	--

Section 4: Purpose of the System4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input checked="" type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input checked="" type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

This PII and BII data is collected by the USPTO to enable identification of the inventory and facilitate the patent application process. DCL does not store any data. After receiving and processing data it is directly transmitted back to USPTO. The PII/BII comes from persons applying for patents through the USPTO. This could include federal employees, contractors, members of the public, or foreign nationals.

- 5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Nation states and adversarial entities are the predominant threats to the information collected and its privacy. The system has implemented security controls following NIST guidance to deter and prevent threats to privacy.

Safeguards employed by the DCL system are: Physically secured and closely monitored. Only individuals authorized are granted logical access. All patent information is encrypted when transferred between DCL and USPTO using secure electronic methods. Periodic security testing is conducted to help assure that any new security vulnerabilities are discovered and fixed. All personnel are trained to securely handle patent information and to understand their responsibilities for protecting patents.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	---

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input checked="" type="checkbox"/>	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>NSI and PCAPS-IP – EFSWeb - Access controls, auditing and encryption are leveraged to prevent PII/BII leakage.</p>
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

- 6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
Other (specify):			

Section 7: Notice and Consent

- 7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and
-------------------------------------	--

	discussed in Section 9.	
<input type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _____.	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: DCLPS depends on the notice provided at the time of collection by PCAPS-IP EFSWeb
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: DCLPS depends on the notice provided at the time of collection by PCAPS-IP EFSWeb
<input type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: DCLPS depends on the notice provided at the time of collection by PCAPS-IP EFSWeb The information is volunteered by individuals as a part of the patent application process. The PII/BII contained in this information is needed for successful processing of the patent application.
<input type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: During patent submission via EFSWeb, applicants have opportunities to update PII/BII data prior to final submission. After a patent submission, users must contact the Electronic Business Center for PII updates. All subsequent BII updates occur within PCAPS-ES system.
<input type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

<input checked="" type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: File level auditing records the user accounts that access all files.
<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>March 31, 2019</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input checked="" type="checkbox"/>	Contracts with customers establish ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	Other (specify):

- 8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. (Include data encryption in transit and/or at rest, if applicable).

DCLPS employs NIST recommended controls to protect PII/BII. Physical and logical access controls are in place to permit access to authorized users, monitored auditing, user training, encryption at transmission and rest are used.

Section 9: Privacy Act

- 9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (A new system of records notice (SORN) is required if the system is not covered by an existing SORN).

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (list all that apply): Patent Application Files—PAT/TM—7 http://www.uspto.gov/sites/default/files/sorn/uspto-pasorn-07.pdf
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on (date).

<input type="checkbox"/>	No, this system is not a system of records and a SORN is not applicable.
--------------------------	--

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: Patent Examination Working Files (N1-241-10-1:4.2)
<input type="checkbox"/>	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.
(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels.
(Check all that apply.)

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Occupation, name, title, address, phone number, & email address.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: PII is only on the system for the time it takes to process and return

		to USPTO. This is usually less than four hours.
<input type="checkbox"/>	Data Field Sensitivity	Provide explanation:
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: Information is for identifying and tracking patent applicants/applications.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: Based on the data fields and in accordance with the Privacy Act of 1974, PII must be protected
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: Because the information containing PII must be transmitted outside of USPTO environment, there is an added need to ensure the confidentiality of information during transmission.
<input type="checkbox"/>	Other:	Provide explanation:

Section 12: Analysis

- 12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Nation states and adversarial entities are the predominant threats to the information collected and its privacy. Security controls following FedRAMP and NIST guidance were implemented to deter and prevent threats to privacy.

- 12.2 Indicate whether the conduct of this PIA results in any required business process changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required business process changes.

- 12.3 Indicate whether the conduct of this PIA results in any required technology changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.